REMARKS

Initially, in the Office Action dated October 1, 2004, the Examiner rejects claims 1-14 under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential structural cooperative relationships, steps, such omission amounting to a gap between the necessary structure. Claims 1-14 have been rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1-14 have been rejected under 35 U.S.C. §101. Claims 1-12 have been rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,854,759 (Kaliski Jr. et al.). Claims 13 and 14 have been rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,987,131 (Clapp) in view of Kaliski Jr. et al.

By the present response, Applicant has submitted new claims 15-22 for consideration by the Examiner and submit that these claims do not contain any prohibited new matter. Further, Applicant has amended claims 1-7 and 11 to further clarify the invention. Claims 1-22 remain pending in the present application.

35 U.S.C. §112 Rejections

Claims 1-14 have been rejected under 35 U.S.C. §112, second paragraph. Applicant has amended the claims of the present application to clarify the invention and respectfully request that these rejections be withdrawn.

35 U.S.C. §101 Rejections

Claims 1-14 have been rejected under 35 U.S.C. §101. Applicant has amended the claims of the present invention to further clarify the invention and respectfully request that these rejections be withdrawn.

35 U.S.C. §102 Rejections

Claims 1-12 have been rejected under 35 U.S.C. §102(b) as being anticipated by Kaliski Jr. et al. Applicant respectfully traverses these rejections.

Kaliski Jr. et al. discloses methods and apparatus for converting a value A representing in a first basis an element of a finite field $GF(q^m)$ to a value B representing the element in a second basis, where q is a prime number or power of a prime number and m is an integer greater than or equal to 2, and where the value B includes a vector of m coefficients from a finite field GF(q). An exemplary apparatus, particularly well-suited for exporting the value A in an internal basis representation to the value B in an external basis representation, includes an externally shifted sequence generator for generating from the value A a sequence of intermediate values representing in the first basis elements of the finite field $GF(q^m)$ whose representations in the second basis are related to the value B by a predetermined external shift operation. An extractor coupled to the externally shifted sequence generator receives and processes the sequence of intermediate values to generate each coefficient of the value B.

Regarding claims 1-7 and 11, Applicant submits that Kaliski Jr. et al. does not disclose or suggest the limitations in the combination of each of these claims of, inter

alia, executing operations on an elliptic curve a predetermined number of times and in a predetermined order without depending on a determined value of the bit of a scalar value to calculate a scalar multiplied point where the operations include calculations of addition and doubling, the operations being selected for scalar values of one or zero and the scalar value determining the selection of the addition and doubling calculations executed. According to the present invention, the addition and doubling are executed for each case of scalar value 1 or 0. By this processing, the power consumption is usually the same in both cases of scalar values 1 or 0, therefore, the elliptic curve cryptosystem cannot be analyzed. In contrast, Kaliski Jr. et al. discloses a general elliptic curve cryptosystem where doubling or addition is executed according to a bit value where if the power consumption is analyzed, the timing when the addition or doubling was executed can be revealed. Kaliski Jr. et al. does not disclose or suggest where the operations are selected for scalar values of 1 or 0 where the scalar value determines the selection of the addition and doubling calculations executed. Kaliski Jr. et al. merely relates to techniques for converting signals for a finite field having one basis two signals of a finite field having another basis using finite field basis conversion techniques which are suitable for use with a number of different types of bases.

Regarding claims 8-10 and 12, Applicant submits that these claims are dependent on one of independent claims 1-7 and 11 and, therefore, are patentable for the same reasons noted regarding these independent claims. For example, Applicant submits that Kaliski Jr. et al. does not disclose or suggest a data

generation method for generating second data from first data that includes calculating a scalar multiplication by use of a scalar multiplication calculation method or signature generation for generating signature data from data that includes calculating a scalar multiplication by use of a scalar multiplication calculation method.

Accordingly, Applicant submits that Kaliski Jr. et al. does not disclose or suggest the limitations in the combination of each of claims 1-12 of the present application. Applicant respectfully requests that these rejections be withdrawn and that these claims be allowed.

35 U.S.C. §103 Rejections

Claims 13 and 14 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Clapp in view of Kaliski Jr. et al. Applicant respectfully traverses these rejections.

Clapp discloses a public-key method of cryptographic key exchange using modular exponentiation in which memory, for storing pre-computed results can be flexibly traded off against the computational complexity of key-exchange. Typically, key exchange is performed by the method of Diffie-Hellman but with exponents having a constrained form such that by use of small table of pre-computed powers of a users public key, any possible shared secret key within the allowed set can be computed with many fewer modular multiplications than the number of bits of effective key-length thereby obtained. The table of pre-computed powers is transmitted as part of the key exchange protocol.

Applicant submits that claims 13 and 14 are dependent on one of independent claims 1-7 and, therefore, are patentable for the same reasons noted previously regarding these independent claims. Applicant submits that Clapp does not overcome the substantial defects noted previously regarding Kaliski Jr. et al. For example, Applicant submits that none of the cited references disclose or suggest a scalar multiplication calculation method wherein a Montgomery-form elliptic curve is used as the elliptic curve, or where an elliptic curve defined on a finite field of characteristic 2 is used as the elliptic curve.

Accordingly, Applicant submits that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 13 and 14 of the present invention. Applicant respectfully requests that these rejections be withdrawn and that these claims be allowed.

New Claims

Applicant has submitted new claims 15-22 for consideration by the Examiner, and respectfully submit that these claims are patentable over the cited references. Applicant submits that these claims are dependent on one of independent claims 1-7 and 11 and, therefore, are patentable for the same reasons noted previously regarding these independent claims. For example, Applicant submits that none of the cited references disclose or suggest a multiplication calculation method wherein when the value of the bit of the scalar is 0, the addition calculation includes adding a point mP to a double point of the point (m+1)P and the doubling calculations include

doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and wherein when the value of the bit of the scalar is 1, the addition calculation includes adding a point mP to a double point of the point (m+1)P and the doubling calculations include doubling the double point of the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.

Accordingly, Applicant submits that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of new claims 15-22 of the present application. Applicant respectfully requests that these claims be entered and allowed.

In view of the foregoing amendments and remarks, Applicant submits that claims 1-22 are now in condition for allowance. Early allowance of such claims is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly, Stanger & Malur, P.C., Deposit Account No. 50-1417 (referencing attorney docket no. 500.39908X00).

Respectfully submitted,

MATTINGLY, STANGER & MALUR, P.C.

Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 684-1120